What is claimed is:

1. A file management apparatus that encrypts a plaintext to generate a ciphertext, stores the ciphertext, and decrypts the ciphertext, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration means for encrypting the key information using a password to generate an encrypted key;

encryption means for encrypting a plaintext based on the key information to generate a ciphertext;

switch means for switching between (a) generating key information by decrypting the encrypted key using the password and (b) reading the key information from the key storage medium; and

decryption means for decrypting the ciphertext based on one of the generated key information and the read key information.

2. The file management apparatus of Claim 1 further comprising a memory unit,

wherein the registration means receives an input of the password, encrypts the key information using the received password to generate the encrypted key, and writes the generated encrypted key to the memory unit,

the encryption means encrypts the plaintext using a file

key to generate the ciphertext, encrypts the file key using the key information to generate an encrypted file key, and writes the ciphertext in association with the encrypted file key, to the memory unit,

the switch means

(a) includes first key obtaining means for receiving an input of the password and decrypting the encrypted key using the received password to generate the key information, and second key obtaining means for reading the key information from the key storage medium, and

(b) obtains the key information by one of the first key obtaining means and the second key obtaining means, and

the decryption means decrypts the encrypted file key using the obtained key information to generate a file key, and decrypts the ciphertext using the file key to generate a decrypted text.

3. The file management apparatus of Claim 2,

wherein the registration means further receives an input of a user identifier that identifies a user, and writes the user identifier in association with the encrypted key, to the memory unit, and

the first key obtaining means further receives an input of the user identifier and decrypts the encrypted key that is associated with the user identifier.

4. The file management apparatus of Claim 2,

wherein the registration means further writes the key information and/or authentication information in association with the encrypted key, to the memory unit,

the encryption means further writes the encrypted key, the key information, and/or authentication information in association with the ciphertext, to the memory unit,

the first key obtaining means checks, using the authentication information, whether the encrypted key has been altered or not, when the encrypted key that is associated with the authentication information is decrypted, and

the decryption means checks, using the authentication information, whether the ciphertext has been altered or not, when the ciphertext that is associated with the authentication information is decrypted.

5. The file management apparatus of Claim 2,

wherein the registration means writes the encrypted key to the memory unit that is a portable storage medium, and

the first key obtaining means decrypts the encrypted key that has been written to the memory unit that is the portable storage medium.

6. The file management apparatus of Claim 2, further comprising

deletion means for deleting the encrypted key that has been written to the memory unit.

7. The file management apparatus of Claim 2, further comprising

deletion means for deleting the encrypted key that has been written to the memory unit,

wherein the registration means further receives an input of a new password, encrypts the key information using the new password to generate a new encrypted key, and writes the generated new encrypted key to the memory unit.

8. The file management apparatus of Claim 2,

wherein the key storage medium stores new key information beforehand, instead of the key information,

the registration means receives the input of the password and decrypts the encrypted key using the password to generate key information,

the encryption means decrypts the encrypted file key using the key information to generate a file key, encrypts the file key using the new key information to generate a new encrypted file key, and writes the new encrypted file key over the encrypted file key in the memory unit, and

the registration means encrypts the new key information using the password to generate a new encrypted key and writes

the new encrypted key over the encrypted key in the memory unit.

9. The file management apparatus of Claim 8,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with the ciphertext and the encrypted file key, to the memory unit, and

the encryption means retrieves the encrypted file key that is associated with the user identifier in the memory unit and generates a file key from the retrieved encrypted file key.

10. The file management apparatus of Claim 8,

wherein the encryption means further writes encryption information in association with the ciphertext and the encrypted file key, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means retrieves the encrypted file key that is associated with the encryption information in the memory unit, and generates a file key from the retrieved encrypted file key.

11. The file management apparatus of Claim 8,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, and

the encryption means extracts the file identifier that is associated with the user identifier from the unified file, specifies the encrypted file key identified by the extracted file identifier, and generates a file key from the specified encrypted file key.

12. The file management apparatus of Claim 8,

wherein the encryption means further writes encryption information in association with a file identifier that identifies the ciphertext and the encrypted file key, as a unified file, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means extracts the file identifier that is associated with the encryption information from the unified file, specifies the encrypted file key identified by the extracted file identifier, and generates a file key from the specified encrypted file key.

13. The file management apparatus of Claim 2,

wherein the encryption means further writes the encrypted key in association with the ciphertext and the encrypted file key, to the memory unit, and

the first key obtaining means decrypts the encrypted key that is associated with the ciphertext and the encrypted file key.

14. The file management apparatus of Claim 13,

wherein the encryption means further receives an input of an indication, the indication showing whether the encrypted key and the ciphertext are to be written in association with each other to the memory unit, and writes, when the indication shows that the encrypted key and the ciphertext are to be written in association with each other, the encrypted key in association with the ciphertext, to the memory unit.

15. The file management apparatus of Claim 13,

wherein the registration means writes the generated encrypted key to the key storage medium instead of to the memory unit.

16. A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext into a memory unit thereof, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration means for receiving an input of a password, encrypts the key information using the received password to generate an encrypted key, and writes the generated encrypted key to the memory unit; and

encryption means for encrypting a plaintext using a file key to generate a ciphertext, encrypting the file key using the key information to generate an encrypted file key, and writing the ciphertext in association with the encrypted file key, to the memory unit.

17. A file decryption apparatus that stores the ciphertext and the encrypted file key generated by the file encryption apparatus of Claim 16, in association with each other, in a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:

a key storage medium storing key information beforehand;

switch means

(a) including first key obtaining means for receiving an input of a password and decrypting the encrypted key using the received password to generate key information, and second key obtaining means for reading the key information from the key storage medium, and

(b) obtaining the key information by one of the first key obtaining means and the second key obtaining means; and

decryption means for decrypting the encrypted file key using the obtained key information to generate a file key, and decrypts the ciphertext using the file key to generate a decrypted text.

18. A file management apparatus that encrypts a plaintext to generate a ciphertext, stores the ciphertext, and decrypts the ciphertext, the file management apparatus comprising:

a key storage medium storing key information beforehand;

registration means for encrypting a password using the key information to generate an encrypted password;

encryption means for encrypting a plaintext using a file key to generate a ciphertext, encrypting the file key based on a password obtained by decrypting the encrypted password to generate a first encrypted file key, and encrypting the file key based on the key information to generate a second encrypted file key;

switch means for switching between (a) decrypting the first encrypted file key based on the password and (b) decrypting the second encrypted file key based on the key information, to generate a file key; and

decryption means for decrypting the ciphertext using the generated file key.

19. The file management apparatus of Claim 18 further comprising a memory unit,

wherein the registration means receives an input of the password, encrypts the received password using the key information to generate the encrypted password, and writes the generated encrypted password to the memory unit,

the encryption means decrypts the encrypted password using the key information to generate the password, encrypts the plaintext using the file key to generate the ciphertext, encrypts the file key using the password to generate the first encrypted file key, encrypts the file key using the key information to generate the second encrypted file key, and writes the ciphertext in association with the first encrypted file key and the second encrypted file key, to the memory unit,

the switch means

(a) includes first key obtaining means for receiving an input of the password and decrypting the first encrypted fie key using the received password, and second key obtaining means for decrypting the second encrypted file key using the key information, and

(b) obtains the file key by one of the first key obtaining means and the second key obtaining means, and

the decryption means decrypts the ciphertext using the obtained file key to generate a decrypted text.

20. The file management apparatus of Claim 19,

wherein the registration means further receives an input of a user identifier that identifies a user, and writes the encrypted password in association with the user identifier, to the memory unit, and

the encryption means further receives an input of the user identifier and decrypts the encrypted password that is associated with the user identifier.

21. The file management apparatus of Claim 19,

wherein the encryption means receives an input of an indication, the indication showing whether the first encrypted file key is to be generated or not, and

(a) generates, when the indication shows that the first encrypted file key is to be generated, the first encrypted file key, and

(b) suppresses, when the indication shows that the first encrypted file key is not to be generated, both generating and writing of the first encrypted file key.

22. The file management apparatus of Claim 19,

wherein the registration means further writes authentication information in association with the encrypted password, to the memory unit,

the encryption means further checks, using the

authentication information, whether the encrypted key has been altered or not, when the encrypted key is decrypted, and

the encryption means further writes the authentication information in association with each of the first encrypted file key, the second encrypted file key, and the ciphertext, to the memory unit,

the first key obtaining means and the second key obtaining means each check, using the authentication information associated with the first encrypted file key and the second encrypted file key, whether the first encrypted file key and the second encrypted file key have been altered or not, when the first encrypted file key and the second encrypted file key are decrypted, and

the decryption means checks, using the authentication information that is associated with the ciphertext, whether the ciphertext has been altered or not, when the ciphertext is decrypted.

23. The file management apparatus of Claim 19,

wherein the registration means writes the encrypted password to the key storage medium, instead of to the memory unit, and

the encryption means decrypts the encrypted password that has been written to the key storage medium.

24. The file management apparatus of Claim 19,

wherein the registration means further receives an input of a new password, encrypts the new password using the key information to generate a new encrypted password, and writes the generated new encrypted password over the encrypted password in the memory unit, and

the encryption means decrypts the second encrypted file key using the key information to generate a file key, encrypts the file key using the new password to generate a new first encrypted file key, and writes the new first encrypted file key over the first encrypted file key in the memory unit.

25. The file management apparatus of Claim 24,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with the ciphertext, the first encrypted file key, and the second encrypted file key, to the memory unit, and

the encryption means retrieves the second encrypted file key that is associated with the user identifier, and decrypts the retrieved second encrypted file key.

26. The file management apparatus of Claim 24,

wherein the encryption means further writes encryption

information in association with the ciphertext, the first encrypted file key, and the second encrypted file key, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means retrieves the second encrypted file key that is associated with the encryption information, and decrypts the retrieved second encrypted file key.

27. The file management apparatus of Claim 24,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with a file identifier that identifies the ciphertext, the first encrypted file key, and the second encrypted file key, as a unified file, to the memory unit, and

the encryption means extracts the file identifier that is associated with the user identifier from the unified file, specifies the second encrypted file key identified by the extracted file identifier, and decrypts the specified second encrypted file key.

28. The file management apparatus of Claim 24,

wherein the encryption means further writes encryption information in association with a file identifier that

identifies the ciphertext, the first encrypted file key, and the second encrypted file key, as a unified file, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means extracts the file identifier that is associated with the encryption information from the unified file, specifies the second encrypted file key identified by the extracted file identifier, and generates a file key from the specified second encrypted file key.

29. The file management apparatus of Claim 19 further comprising

deleting means for deleting the second encrypted file key that has been written to the memory unit.

30. The file management apparatus of Claim 19,

wherein the key storage medium stores new key information beforehand, instead of the key information,

the registration means receives the input of the password and decrypts the received password using the new key information to generate a new encrypted password, and writes the generated new encrypted password over the encrypted password in the memory unit, and

the encryption means decrypts the first encrypted file key using the password to generate a file key, encrypts the

file key using the new key information to generate a new second encrypted file key, and writes the new second encrypted file key over the second encrypted file key in the memory unit.

31. The file management apparatus of Claim 30,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with the ciphertext, the first encrypted file key, and the second encrypted file key, to the memory unit,

the encryption means retrieves the first encrypted file key that is associated with the user identifier and decrypts the retrieved first encrypted file key.

32. The file management apparatus of Claim 30,

wherein the encryption means further writes encryption information in association with the ciphertext, the first encrypted file key, and the second encrypted file key, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means retrieves the first encrypted file key that is associated with the encryption information and decrypts the retrieved first encrypted file key.

33. The file management apparatus of Claim 30,

wherein the registration means further receives an input of a user identifier that identifies a user,

the encryption means further writes the user identifier in association with a file identifier that identifies the ciphertext, the first encrypted file key, and the second encrypted file key, as a unified file, to the memory unit, and

the encryption means extracts the file identifier that is associated with the user identifier from the unified file, specifies the first encrypted file key identified by the extracted file identifier, and decrypts the specified first encrypted file key.

34. The file management apparatus of Claim 30,

wherein the encryption means further writes encryption information in association with a file identifier that identifies the ciphertext, the first encrypted file key, and the second encrypted file key, as a unified file, to the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the encryption means extracts the file identifier that is associated with the encryption information from the unified file, specifies the first encrypted file key identified by the extracted file identifier, and generates a file key from the specified first encrypted file key.

35. The file management apparatus of Claim 19,

wherein the switch means further receives an input of the password, decrypts the first encrypted file key using the received password to generate a first file key, decrypts the second encrypted file key using the key information to generate a second file key, judges whether the first file key and the second file key match, and detects an error when the first file key and the second file key do not match.

36. A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext in a memory unit thereof, the file encryption apparatus comprising:

a key storage medium storing key information beforehand;

registration means for receiving an input of a password, encrypts the received password using the key information to generate an encrypted password, and writes the generated encrypted password to the memory unit; and

encryption means for decrypting the encrypted password using the key information to generate a password, encrypts a plaintext using a file key to generate a ciphertext, encrypts the file key using the password to generate a first encrypted file key, encrypts the file key using the key information to generate a second encrypted file key, and writes the ciphertext in association with the first encrypted file key and the second encrypted file key, to the memory unit.

37. A file decryption apparatus that stores the ciphertext, the first encrypted file key, and the second encrypted file key generated by the file encryption apparatus of Claim 35, in association with each other, in a memory unit thereof, and decrypts the ciphertext, the file decryption apparatus comprising:

a key storage medium storing key information beforehand;

switch means

(a) including first key obtaining means for receiving an input of a password and decrypting the first encrypted fie key using the received password, and second key obtaining means for decrypting the second encrypted file key using the key information, and

(b) obtaining a file key by one of the first key obtaining means and the second key obtaining means, and

decryption means for decrypting the ciphertext using the obtained file key to generate a decrypted text.